

# STOP MANIPULACJI, nie daj się oszukać!













www.niedajmysieoszukac.pl

#### Organizatorzy











#### Trwające kampanie

























#### Patroni honorowi







































## Współfinansowanie





#### **ONAS**



**STOWARZYSZENIE MANKO** od 10 lat pod Patronatem Honorowym i we współpracy m.in. z Ministerstwem Rodziny i Polityki Społecznej, Ministerstwem Zdrowia, Ministerstwem Sportu i Turystyki, Sejmową Komisją Polityki Senioralnej oraz wieloma innymi instytucjami zajmuje się polityką senioralną i wspieraniem osób starszych - ich edukacją i aktywizacją. Nasze działania z sukcesem prowadzimy na terenie całej Polski i za granicą.

Ogólnopolską Kartę Seniora posiada już ponad 450 tysięcy seniorów, honoruje ją 2600 punktów, a ponad 180 gmin przystąpiło do naszego Programu Gmina Przyjazna Seniorom i wydało z nami lokalną edycję Ogólnopolskiej Karty Seniora, która działa w danej miejscowości i całej Polsce. Magazyn Ogólnopolski Głos Seniora o nakładzie 30 tys. egzemplarzy dociera już do ponad 800 organizacji seniorskich w Polsce i za granicą. Nasi przedstawiciele zasiadają w Radzie do spraw Polityki Senioralnej przy Ministerstwie Rodziny i Polityki Społecznej, Radzie Organizacji Pacjentów przy Rzeczniku Praw Pacjenta oraz Radzie Dostępności przy Ministerstwie Funduszy i Polityki Regionalnej.

#### **O KAMPANII**



Na oszustwa najczęściej narażeni są seniorzy mieszkający samotnie, bez rodziny, którzy dają się zwieść różnorodnym i coraz to nowszym metodom naciągania i manipulacji. Przeciwdziała temu **Stowarzyszenie MANKO – Głos Seniora**, które edukuje w zakresie prawa i bezpieczeństwa osób starszych. Od 5 lat uświadamia i przestrzega seniorów, przed manipulacją i demaskuje najnowsze techniki oszustw. W tym roku stowarzyszenie zainaugurowało już IV edycję kampanii "**BEZPIECZNY SENIOR – STOP MANIPU-LACJI, NIE DAJ SIĘ OSZUKAĆ"**, którą prowadzi we współpracy z Ministerstwem Rodziny i Polityki Społecznej. Ponadto w kampanię zaangażowane są także miasta partnerskie, prawnicy, Policja czy Urząd Komunikacji Elektronicznej. Jak wynika z oficjalnych danych rocznie przestępcy dzięki różnego rodzaju oszustwom wyciągają z kont bankowych seniorów ponad **85 milionów złotych**. Dlatego edukacja osób starszych w obszarze bezpieczeństwa jest tak potrzebna.

# SENIORZE, NIE DAJ SIĘ OSZUKAĆ!

W czasie pandemii seniorzy są nie tylko narażeni na wirusy, ale także na nieetyczne praktyki biznesowe. Od marca 2020 roku przestępcy dwoją się i troją, aby wykorzystać lęk, panikę i izolację seniorów w Polsce. Wszechobecny lęk, szczególnie wśród osób w wieku 60+, skrzętnie wykorzystują manipulatorzy na wielu płaszczyznach. Działają w Internecie, ale też w kontakcie bezpośrednim.

W publikacji przedstawimy najnowsze metody oszustw. Skupimy się zarówno na tych aktualnych jak i najbardziej powszechnych. Pamiętajmy, że choć oszustwa różnią się od siebie opierają się na bardzo podobnych mechanizmach. Jeżeli będziesz znał metody oszustw, techniki manipulacji oraz tricki sprzedażowe staniesz się bardziej wyczulony na niepokojące zjawiska w sieci jak i poza nią. **Stop manipulacji-nie daj się oszukać!** 



#### **SPOOFING**

**Spoofing** jest jednym z częściej stosowanych przez cyberprzestępców mechanizmów, mających na celu **wyłudzanie poufnych danych.** Zjawisko polega na dostarczaniu fałszywych maili, smsów łudząco podobnych do wiadomości wysyłanych przez firmy i instytucje które znamy i które budzą zaufanie, np. banki, urzędy czy firmy kurierskie.



#### Na czym polega spoofing?

- 1. Przestępcy wysyłają maila lub SMS'a niemal identycznego do tego, jaki nadaje prawdziwy nadawca, np. firma przewozowa, poczta, dostawca gazu czy prądu.
- 2. Po kliknięciu we wskazany w wiadomości link, ofiara zostaje przeniesiona pod **fałszywy adres**, strony łudząco podobnej wizualnie do oryginału. Tam, w celu rzekomej weryfikacji użytkownik proszony jest o podanie swoich danych, np. imienia i nazwiska, adresu, hasła, numery karty kredytowej, numeru telefonu czy numeru dokumentu tożsamości, bądź innego numeru służącego identyfikacji. Prócz wyłudzenia danych, w trakcie ataku komputer zostaje zainfekowany wirusem, który przejmuje kontrolę nad sprzętem i pozwala na podszywanie się pod użytkownika w trakcie różnych działań w sieci czy wysyłanie w jego imieniu korespondencji mailowej. Właśnie ten element zainfekowania wirusem odróżnia spoofing od phishingu, który ma na celu wyłącznie uzyskanie danych poufnych użytkownika.

#### PAMIĘTAJ!

Zachowaj zdrowy rozsądek! Nie klikaj w podejrzane linki. Pokaż je swojej wnuczce, córce czy sąsiadce. Zainstaluj aktualizacje systemowe i oprogramowanie antywirusowe. Sprawdzaj nagłówki wiadomości mailowych oraz adresy email, z których przychodzą. W razie wątpliwości skontaktuj się z potencjalnym nadawcą bezpośrednio - zadzwoń na oficjalny numer banku, urzędu czy firmy kurierskiej.

#### **PHISHING**

**PHISHING** jest przebiegłą metodą oszustwa internetowego, za którego pośrednictwem przestępca podszywa się pod jakąś instytucję lub osobę. Phishing nosi również inną nazwę: password harvesting fishing. To tzw. **łowienie haseł**, którego celem jest wykradanie numerów kart kredytowych, haseł do logowania oraz innych poufnych informacji za pośrednictwem różnego rodzaju technik. Różni się od spoofingu tym, że nie infekuje twojej komórki bądź komputera złośliwym wirusem, a podstępnie skłania do podania poufnych informacji tj. hasło do bankowości internetowej czy numer karty kredytowej.



#### Na czym polega?

- 1. Przestępca tworzy kopie strony internetowej wybranej instytucji (zazwyczaj finansowej) np. www.adresbanku.pl/logowanie, www.adresbanku-logowanie.pl
- 2. Przestępca wysyła wiadomości e-mail, pochodzące rzekomo z banku, urzędu czy innej instytucji. Wiarygodność zdobywa wykorzystując prawdziwe logo, styl biznesowy firmy.
- 3. Przestępca za pomocą formularza próbuje Cię nakłonić do ujawnienia swoich danych (login, hasło, PIN, dane karty kredytowej).

#### PAMIĘTAJ!

Zanim wpiszesz wrażliwe dane na stronie internetowej, dokładnie sprawdź jej adres URL. Sprawdź czy jest to prawdziwa witryna? Czy adres zawiera jakieś dodatkowe litery? Czy niektóre litery zostały zamienione na cyfry, np. O na 0? Bądź ostrożny!

#### **SMISHING**

**SMISHING** to SMS-owa wersja oszustw phishingowych. Zamiast fałszywej wiadomości e-mail na smartfonie otrzymasz fałszywą wiadomość tekstową. Oszuści najczęściej próbują nakłonić nas do kliknięcia w link w celu wykonania drobnej dopłaty (kilka złotych), aby np. nie dokonano nam blokady numeru telefonu z uwagi na drobną niedopłatę. Oczywiście powody, aby kliknąć w link, mogą być różne: zaległość w urzędzie skarbowym, uzyskanie kodu odbioru paczki, niedopłata za mandat, niedopłata za prąd czy gaz. Po kliknięciu w przesłany link będziemy przekierowani do nieprawdziwych stron banku czy fałszywych stron szybkiej płatności.

**Efekt?** Możemy stracić w ten sposób dane do logowania, czyli w konsekwencji pieniądze lub zainstalować aplikację, która będzie miała dostęp do telefonu wraz z SMS-kodami, którymi często potwierdzamy transakcje bankowe.

Twoja faktura nie została w pełni opłacona. Prosimy o dopłatę 1 zl do dnia 22.11.2021 pod linkiem bit.ly/zhshs lub twój numer zostanie zablokowany.

1 14:29

#### **VISHING**

**VISHING** to wyłudzenia danych poprzez rozmowę telefoniczną. Dzwoniący podaje się za pracownika naszego banku, doradcę inwestycyjnego, instytucję zaufania publicznego i prowadzi rozmowę w taki sposób, że ofiara ujawnia swoje poufne dane. W międzyczasie albo chwilę po rozmowie telefonicznej konto ofiary zostaje opróżnione, a bardzo często także obciążone kredytem na wiele tysięcy złotych.

#### **OSZUSTWO NA TELEFON ZZA GRANICY**

**WANGIRI FRAUD** to metoda wyłudzenia pieniędzy wykorzystująca połączenia telefoniczne. Dzwoniący posługują się zagranicznymi numerami telefonów, by nakłonić do kontaktu, który może wiązać się z wysokimi kosztami dla abonenta.

# +<u>223</u> 76 89 26 77 Mali

#### Jak nie dać się oszukać?

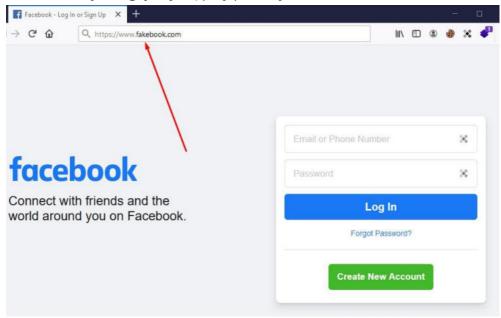
- → **Spójrz na długość ciągu cyfr.** Podejrzanie długi numer telefonu to pierwsza rzecz, na którą powinieneś zwrócić uwagę.
- → **Sprawdź numer dzwoniącego.** Polskie numery telefonów zaczynają się od +48, 0048 albo nie posiadają krajowego numeru kierunkowego wówczas składają się z 9 cyfr.
- Uważaj na to jak długo trwała próba połączenia. Alarmujący powinien być dla Ciebie krótki czas oczekiwania na rozmowę.
- → Zwróć uwagę na porę. Szczególną ostrożność powinny wzbudzić połączenia w godzinach nocnych.
- → NIE ODBIERAJ I NIE ODDZWANIAJ! Reakcja na połączenie wiąże się zazwyczaj z automatycznym przełączeniem na drogą linię "premium", co znacznie obciąży twój rachunek.

#### Co zrobić, jeżeli odebrałeś połączenie?

- → Rozłącz się jak najszybciej! Zminimalizuje to ryzyko większej opłaty telekomunikacyjnej.
- → Zabezpiecz się i zminimalizuj potencjalne straty! Zablokuj dany numer i dodaj go w ustawieniach urządzenia do tzw. czarnej listy. O zdarzeniu pilnie poinformuj operatora swojej sieci.

#### **FACEBOOK PHISHING**

**Facebook** stał się popularnym celem oszustów z dwóch powodów. Przestępca, który zdobędzie dostęp do naszego konta, ma możliwość wykorzystania go do ataków na naszych znajomych. Może także za pomocą naszego konta zalogować się do innych serwisów. **Dlaczego?** Haker po zdobyciu dostępu do naszego konta zyskuje automatycznie dostęp do wszystkich kont, do których logujemy się przy pomocy FB.



#### Na czym polega Facebook phishing?

Zwykle dostajemy e-maila podszywającego się pod Facebook'a, zawierającego link do strony logowania. Strona jest fałszywa i dane, które wprowadziliśmy (login oraz hasło), wędrują prosto do hakera.

#### PAMIĘTAJ!

Nigdy nie klikaj w żadne podejrzane linki. Nazwę strony zawsze wpisuj samodzielnie: www.facebook.com. Wtedy możemy być pewni, że nasze konto jest bezpieczne.

#### **OSZUSTWO NA BLIKA**

**BLIK** to polski system płatności mobilnych. Jest bardzo łatwy w obsłudze, co uporczywie wykorzystują przestępcy na portalach społecznościowych. Oszustwo na BLIKA polega na wyłudzeniu kodu do płatności przez telefon. Osoba logując się do swojego banku, musi wygenerować w aplikacji kod do płatności telefonem, a następnie

Hej, masz może BLIKa? Proszę opłać moje zamówienia, oddam ci z nawiązką. Potrzebuję 500 zł. Jutro oddam!



Cześć, jasne nie ma problemu.

Podasz mi kod BLIK z aplikacji bankowej??



samodzielnie go wykorzystać bądź przesłać go "znajomemu". Niestety w przeciwieństwie do płatności przelewem, transakcji dokonanych za pomocą tego kodu nie można już cofnąć, gdyż przestępca od razu wpisuje podany kod BLIK w bankomacie i wypłaca z niego pieniądze.

#### Co zrobić aby uchronić się przed oszustwem?

- → Stosuj dwuskładnikowe uwierzytelnienie swoich kont społecznościowych
- → Zweryfikuj tożsamość znajomego najlepiej zadzwoń do niego.
- → Chroń swój PIN do aplikacji bankowej.

#### **FAŁSZYWE BILETY KONCERTOWE**

Do tego oszustwa przestępcy wykorzystują system wydarzeń na facebook'u. Oszustwo polega na utworzeniu wydarzenia, na które bilety zostały wyprzedane. Następnie fałszywe wydarzenie jest promowane za niewielką kwotę finansową. Ruch ze strony wydarzenia kierowany jest na fałszywą stronę sprzedaży biletów. Po zakupie okazuje się, że bilet nie istnieje, a pieniądze są nie do odzyskania.

#### PAMIĘTAJ!

Korzystaj tylko z oficjalnych stron sprzedaży biletów tj. www.eventim.pl, www.biletomat.pl

# "ZOBACZ KTO WIDZIAŁ TWÓJ PROFIL"

Oszustwo po raz kolejny ma na celu wyłudzenie poufnych danych. Przestępca wysyła nam linka do pobrania aplikacji, pod którą możesz zobaczyć kto podglądał twój profil. Następnie poprzez aplikację zyskuję twoje hasło i login do facebook'a.

#### PAMIĘTAJ!

Nie ma możliwości sprawdzenia kto odwiedzał Twój profil na Faceboku!

# FAŁSZYWE PROFILE I NEWSY NA FACEBOOK'U

**SCAM** to oszustwo, polegające na tworzeniu fałszywych informacji i profili na facebook' u w celu wzbudzeniu czyjejś ciekawości w konkretnym celu, np. pozyskania danych lub wyłudzenia pieniędzy.



2miliony wyświetleń

#### Tragedia! Znany aktor się powiesił!

Funkcjonariusze zabezpieczyli miejsce zdarzenia. Kliknij i dowiedz się więcej...

#### Jak zidentyfikować SCAM post?

- → Post posiada szokujący, intrygujący, absurdalny tytuł, a także zdjęcie, które ma zwrócić naszą uwagę.
- → Post posiada krótki komentarz typu "Nie wierzę", "To nie możliwe", "Zobacz sam! To jest szokujące", który ma podsycić naszą ciekawość.
- → Oszuści w tym przypadku wykorzystują także autorytet często nazwy ich stron są zbliżone do tych nam znanych np. centrum-wiadomosci24.pl, tvnnewsy24.pl, polsat24h.pl

#### **OSZUSTWO NA SPADEK**



"NA SPADEK" – to wersja oszustwa nigeryjskiego oparta na długotrwałej grze psychologicznej. Ten rodzaj oszustwa zwykle ma postać oficjalnego e-maila lub listu od osoby podającej się za prawnika (czasami z zagranicy), w którym informuje się, że osoba, o takim samym nazwisku jak Ty umarła, a swój ogromny majątek w pozostawionym testamencie przekazała Tobie. Fortunę ofiara może podjąć w banku po dopełnieniu kilku formalności i opłaceniu różnych należności, które są niczym w porównaniu z olbrzymim spadkiem. Podobnie, jak w przypadku innych oszustw nigeryjskich, oszuści uwiarygodniają całą historię przesyłając pocztą elektroniczną spreparowane certyfikaty i kopie potwierdzeń przelewów.

#### PAMIĘTAJ!

Jeżeli ktoś proponuję Ci dużą kwotę pieniędzy, bądź pewny, że to oszustwo. Nigdy nie udostępniaj wrażliwych danych, takich jak PESEL, czy skan dowodu osobistego, haseł do bankowości, PIN-ów. Jeśli ktoś za przekazanie nam jakiejś kwoty pieniędzy żąda opłat manipulacyjnych, powinno to wzbudzić nasze wątpliwości.

# AMERYKAŃSKI ŻOŁNIERZ MÓWI "KOCHAM CIĘ"

Oszuści nie mają żadnych skrupułów. Popularną metodą wśród przestępców jest oszustwo na tak zwanego "amerykańskiego żołnierza". Oszust wyszukuje w Internecie samotne osoby, po czym nawiązuje z nimi kontakt. Posługując się zdjęciami z Internetu, przedstawia się jako amerykański żołnierz, który aktualnie jest na misji poza granicami swojego kraju. Oszust poprzez regularny kontakt i przedstawienie fałszywych historii z życia zdobywa zaufanie ofiary, a następnie prosi o pomoc finansową na zakup biletu lub bardzo drogie leczenie. Gdy ofiara oszustwa prześle pieniądze na konto przestępcy, zostaje bez ukochanego i bez pieniędzy. Ostatnio pojawiły się także oszustki podające się za "lekarki z amerykańskiej armii". Te z kolei wyłudzają pieniądze od mężczyzn.



# Gen John E Hyten



#### **PAMIĘTAJ!**

Zachowaj szczególną ostrożność w kontaktach z osobami poznanymi przez Internet - nigdy nie mamy pewności, kto znajduje się po drugiej stronie monitora.

# **OSZUSTWO NA NIEISTNIEJĄCEGO PIESKA**

Coraz częściej na różnych portalach internetowych typu Olx lub Allegro dochodzi do przestępstw, a jednym z przykładów jest np. **oferta oddania rasowego psa lub kota z zagranicy, za darmo.** Oszust, do którego zwraca się klient, zapewnia, że zwierzę posiada wszystkie potrzebne szczepienia, dokumenty i rodowód, a za jego przewóz ma być odpowiedzialna agencja specjalizująca się w transporcie zwierząt. Jedyne co klient musi zrobić, to zapłacić za koszty transportu, po dokonaniu rezerwacji wybranego kota lub psa. Agencja wysyła mail z informacją o metodzie płatności: pieniądze należy przesłać za pośrednictwem banku Western Union do Kamerunu, w którym mieści się dyrekcja generalna agencji. Po dokonaniu wpłaty wysyłany jest kolejny mail informujący o tym, że zwierzę musi przejść dodatkowe płatne szczepienia i jeśli klient nie uiści opłaty, trafi ono na dwumiesięczną kwarantannę. I tak zaczyna się spirala wyciągania pieniędzy na nieistniejącego słodkiego szczeniaka czy kotka, rzekomo czekającego na naszą decyzję na lotnisku.



#### PAMIĘTAJ!

Internet to ogrom możliwości, ale również zagrożeń. Bądź świadomy – sprawdź, zastanów się i nie licz na niesamowite okazje! Pamiętaj – schroniska są pełne zwierzaków, które można przygarnąć zupełnie za darmo.

#### **FAŁSZYWE INWESTYCJE W INTERNECIE**



Hasło: "Inwestycja z gwarancją szybkiego zysku, bez wychodzenia z domu" brzmi podejrzanie, jednak wciąż są ludzie, którzy wierzą w takie oferty! Firma "X" zamieszcza swoją reklamę w Internecie. Oferuje inwestycje kapitału w euro w m.in. złoto. Przedsięwzięcie najczęściej jest promowane przez znaną osobę (zdjęcie wykorzystane bez zgody tej osoby) – co wzbudza ciekawość odbiorcy. Oszust kontaktuje się z ofiarą i namawia, do zainwestowania pieniędzy, argumentując, że inwestycja jest bardzo korzystna. Po zainwestowaniu pieniędzy, ofiara nigdy nie dostaje zwrotu zainwestowanych pieniędzy, ani zysków. W innym wariancie oszustwa, ofiara początkowo dostaje na konto niewielkie zyski, aby upewnić ją, że przedsięwzięcie jest legalne.

#### **PAMIĘTAJ!**

Nigdy nie wierz w złudne obietnice szybkiego zarobku w krótkim czasie. Najczęściej zamiast otrzymania pieniędzy, znikają one z naszego konta!

#### **OSZUSTWO NA ELEKTRYKA**



Jednym z najpowszechniejszych oszustw jest metoda na pracownika zakładu energetycznego, gazowni, bądź administracji budynku. Oszuści dzwoniąc do drzwi seniorów twierdzą, że w bloku jest zwarcie, wyciek gazu lub sąsiad z dołu ma zalane mieszkanie. Po okazaniu fałszywych identyfikatorów i dokumentów sprawdzają gniazdka, piecyki gazowe, przewody wentylacyjne, zawory z gazem i wodą. Proponują naprawę "wadliwego" sprzętu i instalacji za wygórowaną kwotę, a podczas sprawdzania mieszkania kradną cenne rzeczy takie jak np. biżuteria. Niejednokrotnie proszą o podpisanie dokumentów i podanie wrażliwych danych co jest wymagane w przypadku dokumentów administracyjnych. Często oszuści podszywają się pod pracowników dotychczasowego dostawcy energii i przekonują do podpisania umowy, dzięki której rachunek za energię elektryczną będzie mniejszy i rozłożony na comiesięczne raty. Niestety to pułapka dla seniorów, jest to zupełnie inna firma przez co należy płacić większe rachunki, a w dodatku dwa – dla swojego dotychczasowego dostawcy oraz nowego.

#### PAMIETAJ!

Zawsze zachowuj szczególną ostrożność w kontaktach z osobami obcymi, bez względu na to za kogo się przedstawiają i jak są ubrani. Stosuj zasadę ograniczonego zaufania. Nie podpisuj żadnych dokumentów bez ich wcześniejszego przeczytania.

# **OSZUSTWO NA FOTOWOLTAIKĘ**



Wszystkie przestępstwa mają wspólny mianownik - pieniądze. W dobie rozwoju odnawialnych źródeł energii na rynku można znaleźć przedsiębiorstwa, które doradzają i montują tego typu urządzenia. Niestety wśród rzetelnych firm mogą znaleźć się także nieuczciwe. Oszuści mogą próbować skłonić nas do zawarcia umowy, która przyniesie dla nas niekorzystne efekty lub zamontowania dużo większej instalacji umożliwiającej późniejszy montaż klimatyzacji czy elektrycznego źródła ogrzewania. Często to strata pieniędzy wpłaconych na poczet realizacji inwestycji, zaciągnięcie zobowiązania celem pokrycia kosztów zakupu, który nie zostanie zrealizowany, a także przekazanie danych osobowych, które mogą być wykorzystane przez przestępców. Naszą czujność powinna wzbudzić chęć szybkiego podpisania umowy, przewidziany błyskawiczny montaż instalacji oraz korzystniejsza oferta niż u innych wykonawców instalacji.

#### PAMIĘTAJ!

Stosuj teorię ograniczonego zaufania! Bez względu na to, jak korzystnie brzmi oferta w ustach konsultanta, zanim zdecydujecie się na podpisanie umowy, dokładnie prześwietlcie całą firmę. Poproś o pomoc dzieci, wnuki bądź znajomych.

#### **OSZUSTWO NA WNUCZKA**



Dla seniorów rodzina jest najważniejsza, dlatego metoda oszustwa związana z nią jest najpopularniejsza. Pomimo wielu kampanii społecznych i ostrzeżeń ze strony policji czy mediów, seniorzy wciąż dają się nabrać na "wnuczka". W związku z obecną sytuacją pandemiczną ta metoda została zmodyfikowana. Oszust dzwoni z prośbą o jak najszybsze opłacenie jego testów na koronawirusa lub całego leczenia. Senior ma przekazać pieniądze "koledze wnuczka" lub wykonać przelew. Pieniędzy nigdy nie odzyska. Często wykorzystywane są także starsze schematy działania przestępców: na operację wnuczka, który uległ wypadkowi, pieniądze na poczet spowodowanych kosztów, dzięki czemu wnuczek/wnuczka nie trafi do więzienia. W przypadku zaistnienia takiej sytuacji należy zadzwonić do bliskich osób, bądź skontaktować się z policją.

#### PAMIĘTAJ!

Nigdy nie przekazuj pieniędzy osobom, których nie znasz. Nie ufaj osobom, które telefonicznie podają się za krewnych lub ich przyjaciół. O sprawie powiadom Policję (nr. 997 lub 112).

## **OSZUSTWO NA "POGOTOWIE RATUNKOWE"**



Sprawcy tego oszustwa pukają do drzwi i przedstawiają się jako pracownicy "pogotowia ratunkowego". Następnie wchodzą do domów, mówiąc, że przyjechali po pieniądze na zakup krwi potrzebnej do przeprowadzenia operacji syna/córki, który uległ wypadkowi w pracy. Zaskoczone i zdenerwowane ofiary nie zastanawiając się ani przez moment nad potwierdzeniem tych faktów przekazują oszustowi pieniądze.

#### Zanim otworzysz drzwi:

- 1. Spójrz przez wizjer w drzwiach lub przez okno zobacz, kto przyszedł!
- **2.** Jeśli nie znasz odwiedzającego spytaj o cel jego wizyty, zapnij łańcuch zabezpieczający (jeśli zdecydujesz się na otwarcie drzwi), poproś o pokazanie dowodu tożsamości lub legitymacji służbowej. Uczciwej osoby nie zrazi twoja ostrożność i nieufność. Dokumenty sprawdzaj uważnie.
- **3.** W razie wątpliwości umów się na inny termin, sprawdzając uprzednio w administracji osiedla lub odpowiedniej instytucji wiarygodność jego i prawdopodobieństwo wizyty.
- **4.** Jeżeli gość jest natarczywy, zaalarmuj otoczenie i zadzwoń po policję. Zawsze staraj się zapamiętać jak najwięcej szczegółów np. numery i markę samochodu, który ewentualnie przyjechał oraz wygląd odwiedzającego.

# PREZENTACJE SPRZEDAŻOWE DLA SENIORÓW- CZYM SĄ?



Każdego dnia w Polsce odbywa się kilkadziesiąt pokazów i prezentacji sprzedażowych, na których głównie osoby starsze są zachęcane do zakupu produktów wątpliwej jakości i pochodzenia po zawyżonych cenach oraz wprowadzane w błąd na temat ich rzekomego leczniczego działania.

Sprzedaż ta odbywa się poza stałymi punktami sprzedaży detalicznej. Zazwyczaj ma miejsce w domu klienta, podczas prezentacji lub wycieczki zorganizowanej przez przedsiębiorcę. Pokazy organizowane są najczęściej w dobrych, ekskluzywnych hotelach, restauracjach, sanatoriach lub parafiach.

# SPOSOBY ZAPRASZANIA GOŚCI NA POKAZY I PREZENTACJE SPRZEDAŻOWE

- → Telefoniczne/Telemarketing
- → Zaproszenia wysyłane pocztą
- → Ulotki informacyjne
- → Ogłoszenia na klatkach schodowych

# NA CO JESTEŚMY ZAPRASZANI?

- → Darmowe badania (podczas których często zostaje ujawniony problem zdrowotny w rozwiązaniu którego ma pomóc oferowany przez sprzedawcę produkt)
- → Bezpłatne konsultacje ze specjalistami
- → Darmowy masaż
- → Wykłady zdrowotne na temat zdrowego stylu życia, ekologicznego gotowania itp.
- → Odbiór darmowego, "cennego" prezentu typu: żelazko, waga, grill, suszarka, wiertarka, ciśnieniomierz, pulsoksymetr. Zwykle są to jednak drobne upominki, które nijak mają się do tego, o czym był informowany klient. Można je odebrać na końcu trwającej często do 3-4 godzin prezentacji. To wszystko ma zachęcić nas do przyjścia na spotkanie.

Zaproszeni goście nie są najczęściej informowani o jego celu handlowym. Na spotkaniach prezentowane są produkty mające ułatwiać funkcjonowanie w domu, pomóc w utrzymaniu dobrego zdrowia, a także wspomagać leczenie. Gości często wprowadza się w błąd co do właściwości oferowanych produktów. Podczas spotkania często zakazuje się używania telefonów komórkowych.





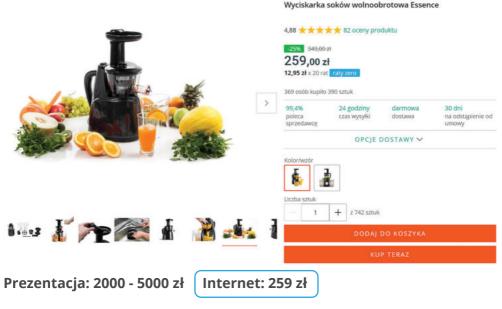
#### PRZEBIEG PREZENTACJI

- → Prezenter to przeważnie elegancka miła, młoda osoba, która kojarzy się z dobrym wnuczkiem
- Swobodna atmosfera, aby klient nie odniósł wrażenia, że cokolwiek będzie sprzedawane
- Każdy ma czuć się wyjątkowo i mieć świadomość, że uczestniczenie w spotkaniu jest okazją i wyróżnieniem
- → Uśmiechy i komplementy w odpowiednich momentach
- → Często osoba prowadząca podaje się za eksperta
- → Prezentacje ilustrowane są filmami z wypowiedziami fachowców i znanych osób
- Często pokazuje się certyfikaty, mające potwierdzać wiarygodność produktu oraz jego wyjątkowość
- → Brawa i oklaski zebranych

#### **DLACZEGO KUPUJEMY NA PREZENTACJACH?**

Podczas prezentacji produktów stosowane są nieznane "zwykłemu" człowiekowi triki handlowe i techniki wywierania wpływu mające podnosić wartość oferowanych produktów i skutecznie przekonać nas do ich zakupu. Za ich pomocą sprzedawcy wywołują w nas potrzebę zakupu oferowanych produktów oraz przekonują nas, że zakup jest rozsądny i opłacalny, nawet jeżeli tak nie jest, a my tak naprawdę go nie potrzebujemy lub nas na niego nie stać.

# PRODUKTY OFEROWANE NA SPOTKANIACH A ICH REALNA CENA /OD 5 DO 50 RAZY WIĘCEJ/





Prezentacja: 6500 zł - 12000 zł | Internet: 219 zł

#### **TECHNIKI MANIPULACJI**



## 1) REGUŁA WZAJEMNOŚCI

Jeśli Ty zrobiłeś dla mnie coś dobrego, to ja także zrobię coś dobrego dla Ciebie. Jesteśmy kuszeni do przyjścia na spotkania rzekomo bezpłatnym prezentem, poczęstunkiem czy badaniami. Podświadomie czujemy się zobowiązani i wdzięczni. A jak tu się odwdzięczyć? Spełnić prośbę i kupić coś od tego kto nas zaprosił. Niestety często w wysokiej i nieuczciwej cenie.

#### 2) SPOŁECZNY DOWÓD SŁUSZNOŚCI

Jeżeli inni ludzie zachowują się w dany sposób, oznacza to że jest on właściwy i ja również będę tak samo postępował. Kiedy podczas prezentacji większość zgromadzonych osób potwierdza, że dany produkt się sprawdza i jest wart swojej ceny, to nie chcemy "wyróżnić się z tłumu" i powiedzieć, że jest wręcz przeciwnie. Przecież wszyscy nie mogą się mylić. Tymczasem Ci, co polecają i przytakują, to osoby zmanipulowane albo podstawione.

#### 3) LUBIENIA I SYMPATII

Jeżeli lubię Ciebie, to chętniej spełnię twoją prośbę. Prezenterzy zawsze częstują nas komplementami i schlebiają nam. Na prezentacjach dowiadujemy się, że mamy na imię jak najukochańsza babcia, żona, siostra czy mama prowadzącego spotkanie. Bądźcie ostrożni przy wszystkich próbach pochlebstw, bo miły i szarmancki nie znaczy uczciwy.



#### 4) WPŁYWU AUTORYTETU

Jeżeli uważam, że jesteś autorytetem, to chętniej spełnię Twoją prośbę. Dlatego często prezenterzy powołują się na opinie ekspertów. Doskonale wiedzą, że podczas prezentacji nie możemy tego sprawdzić i wykorzystują to. Innym przykładem są aktorzy w przebraniu lekarza czy udający znającą się na rzeczy matkę 4 dzieci.

#### 5) NIEDOSTĘPNOŚCI

Tylko tu i teraz. Taka okazja się nie powtórzy. Mamy tyle zamówień, że nie nadążamy z produkcją. Są zapisy i listy rezerwowe. Jeżeli coś jest rzadkie lub trudno osiągalne, to pewnie jest dobre. Najczęściej to wszystko nieprawda. Ma nas skusić do skorzystania z okazji, jaka się już nigdy nie powtórzy. Właśnie z tego powodu często nabieramy się na oferty "last minute", limitowane edycje, okazje, artykuły kolekcjonerskie (im rzadsze tym droższe).

#### 6) ZAANGAŻOWANIA I KONSEKWENCJI

Jeżeli zaangażowałem się w coś, będę kontynuował to działanie, ponieważ chcę być postrzegany jako osoba konsekwentna i nie chcę stracić już zainwestowanego czasu, energii i pieniędzy. Dlatego bardzo często umowy są skonstruowane tak, aby rezygnacja oznaczała stratę tak dużą, że nie opłaca się wycofać.

# TRICKI SPRZEDAŻOWE



#### 1) GRATIS

Do produktu/usługi za określoną cenę dodawany jest gratis mający wywołać wrażenie dodatkowej atrakcji. Działanie to obniża nasze wymagania co do produktu/usługi i spora grupa ludzi jest skłonna skorzystać mimo drobnych wad produktu/usługi, które być może dostrzegła wcześniej.

#### 2) UKRYTE KOSZTY

Najpierw następuję zainteresowanie towarem, a gdy już osoba, której manipulacja bezpośrednio dotyczy, praktycznie zdecyduje się na podpisanie umowy czy kupna towaru, wtedy manipulator zaczyna ujawniać ukryte koszty. Skoro już wystarczająco nakręcił na daną usługę, trudniej będzie z niej zrezygnować mimo ukrytych kosztów.

#### 3) BEZINTERESOWNOŚĆ

Skuteczna metoda, w której ktoś bezinteresownie zachwala produkt np. coś kupujemy a z boku odzywa się niby "przypadkowy przechodzień", który w sposób bezinteresowny pochwala nasz wybór. Kupujemy nie wiedząc, że przechodzień jest podstawiony.

#### 4) METODA "NISKA PIŁKA"

Manipulator przedstawia propozycję, która jest niesamowicie dla nas korzystna. Tuż przed realizacją okazuję się jednak, że nastąpiło nieporozumienie albo pomyłka – towar, o którym była mowa jest droższy.

## 5) WYTWORZENIE W ROZMÓWCY POCZUCIA WYJĄTKOWOŚCI

Przedstawienie konsumenta jako wybrańca losu znanymi wszystkim frazesami tj. "Jest Pani wyjątkowa!", "Jest Pani tego warta!".

#### 6) METODA "DRZWIAMI W TWARZ"

Metoda polegająca na tym, że najpierw wysuwa się bardzo dużą prośbę, a po niej docelową małą, na której zależy manipulatorowi, by została spełniona.



#### **JAK NIE ULEC MANIPULACJI NA PREZENTACJI?**



#### PAMIĘTAJ: LICZY SIĘ CZAS!

Im szybciej podejmiesz działanie, tym lepiej dla Ciebie. Jeżeli jesteś osobą starszą zwróć się o pomoc do swoich dzieci, wnuków, sąsiadów lub znajomych. Osoby młodsze pomogą Ci wybrnąć z sytuacji. Brak działania oznacza często trudne do przewidzenia konsekwencje.

# **PAMIĘTAJ:**

- → Nie ma niczego za darmo!
- → Pośpiech jest złym doradcą. Nie ulegaj pokusie prezentów i promocji. Nie podpisuj niczego bez spokojnego zastanowienia się nad zakupem!
- → Zanim coś kupisz i podpiszesz, poradź się kogoś bliskiego! Czy Twoje dzieci i znajomi również uważają, że produkt jest w dobrej cenie?
- → Porównaj oferty. Poproś dzieci lub wnuki o sprawdzenie w Internecie cen podobnych produktów oraz opinii o firmie organizującej pokaz.
- → Przed zakupem sprzętu medycznego poproś o radę swojego lekarza rodzinnego.
- Przeczytaj uważnie warunki umowy, którą podpisujesz i zażądaj kopii każdego podpisanego przez siebie dokumentu.
- → Nie podpisuj umów, których nie rozumiesz.
- → Nikomu obcemu nie dawaj swojego dowodu osobistego!
- Bądź ostrożny. Często dzieci muszą spłacać kredyty rodziców. Tu chodzi o duże pieniądze!

# CO JEŻELI PODPISAŁEŚ NIEKORZYSTNĄ UMOWĘ I CHCESZ SIĘ Z NIEJ WYCOFAĆ?

Jeżeli podpisałeś umowę na zakup produktów na prezentacji, to w ciągu 14 dni od jej zawarcia możesz z niej zrezygnować bez podania przyczyny.

- Wyślij sprzedawcy oświadczenie o odstąpieniu od umowy (formularz odstąpienia od umowy powinien dostarczyć sprzedawca, wzór pisma znajdziesz również na końcu tego folderu).
- → Poinformuj bank, że rezygnujesz z kredytu, jeśli był on częścią umowy, a towar zakupiłeś na raty.
- Zwróć towar sprzedawcy (rozpakowanie i użycie produktu nie pozbawia Cię prawa do odstąpienia od umowy). Możesz zrobić to osobiście lub wysłać pocztą na adres sprzedawcy.

#### PAMIĘTAJ:

Korespondencję wysyłaj listami poleconymi za potwierdzeniem odbioru.

# **JEŻELI MASZ PROBLEM:**

- → Skorzystaj z pomocy **Powiatowego Rzecznika Praw Konsumenta.**
- Skorzystaj z pomocy prawnika (dowiedz się gdzie w twojej okolicy znajdują się Punkty Nieodpłatnej Pomocy Prawnej).
- → Jeżeli w jakikolwiek sposób czujesz się zagrożony zaistniałą sytuacją, zgłoś problem POLICJI lub w PROKURATURZE (instytucje państwowe są po to, aby Ci pomóc).



# POSTULATY GŁOSU SENIORA - CO JESZCZE NALEŻY ZMIENIĆ

Od 5 lat **Stowarzyszenie Manko – Głos Seniora** apeluje o zmiany prawne ograniczające proceder oszustw i manipulacji na pokazach i prezentacjach sprzedażowych dla Seniorów. Postulujemy o wzmocnienie ochrony konsumentów-seniorów narażonych na karygodne praktyki sprzedażowe m.in. poprzez:

- Wprowadzenie notyfikacji pokazów, czyli zgłoszenia prezentacji 14 dni przed jej planow anym terminem do lokalnego Rzecznika Praw Konsumenta.
- Prowadzenie publicznego rejestru firm prowadzących sprzedaż poza lokalem przedsiębiorstwa (Senior, który chce zwrócić towar, nie wie, gdzie szukać sprzedawcy).
- → **Nakaz rejestrowania video prezentacji** i przechowywania zapisu przez 5 lat
- Wydłużenie okresu rezygnacji z zakupu odstąpienia od umowy kupna-sprzedaży z 14 do 28 dni, aby Senior miał więcej czasu na zorientowanie się w swojej sytuacji.
- Nakaz ujawnienia w zaproszeniu handlowego celu spotkania oraz produktów, które będą sprzedawane, a tym samym wprowadzenie odpowiedzialności karnej za ukrywanie handlowego celu pokazów.



# GŁOS SENIORA NA RZECZ BEZPIECZEŃSTWA SENIORÓW W POLSCE

Ponad 300 warsztatów stacjonarnych, w których wzięło udział ponad 15 000 seniorów







Ponad 30 warsztatów online, z których skorzystało ponad 100 000 Seniorów







15 konferencji prasowych, w wielu miejscach w Polsce







Produkcja i emisja 3 spotów promocyjnych (dotarcie do ponad **2 milionów** Seniorów)







Kilkadziesiąt audycji w mediach ogólnopolskich - TVP, Polsat, Radio Zet itd.







WZÓR 1 Miejscowość, data
Imię i nazwisko konsumenta(-ów) Adres konsumenta(-ów)
Nazwa i adres przedsiębiorcy
Oświadczenie o odstąpieniu od umowy zawartej na odległość lub poza lokalem przedsiębiorstwa
Ja/My (*)niniejszym informuję/informujemy(*) o moim/naszym(*)
odstąpieniu od umowy sprzedaży następujących rzeczy(*)
umowy dostawy następujących rzeczy(*)
umowy o dzieło polegającej na wykonaniu następujących rzeczy/o świadczenie następującej
usługi(*)
Data zawarcia umowy¹/odbioru²(*)
Podpis konsumenta(-ów)

<sup>(\*)</sup> Niepotrzebne skreślić

podać, jeżeli umowa dotyczyła świadczenia usług
 podać, jeżeli umowa dotyczyła zakupu towaru

#### WZÓR 2

	Data, miejscowość:
mię i Nazwisko	
Adres zamieszkania	
Numer PESEL	
eria i numer dowodu osobistego	
Numer klienta	
	Nazwa kredytodawcy
	Adres kredytodawcy
Oświadczam, że na podstawie art. 53 ust.	rawy z dnia 12 maia 2011 r. o kredycie
Oświadczam, że na podstawie art. 53 ust	awy z dnia 12 maja 2011 r. o kredycie
konsumenckim (Dz. U. Nr 126 poz. 715 z p	późn. zm.) odstępuję od umowy kredytu o
numerzezawartej dniaz firm	ıą
	(czytelny podpis)
	(czytemy podpis)

# 10 ZASAD CYBERBEZPIECZEŃSTWA



- 1. Nie otwieraj załączników z niepewnych źródeł i nie klikaj w podejrzane linki.
- 2. Sprawdzaj dokładnie adresy stron www, a także ich certyfikaty.
- 3. Twórz hasła skomplikowane i trudne do odgadnięcia przez postronne osoby.
- **4.** Nie używaj tego samego hasła do różnych kont oraz nie zapisuj haseł na kartkach ani w plikach na komputerze.
- 5. Nie podawaj i nie wysyłaj swoich loginów i haseł innym osobom.
- **6.** Nie loguj się do bankowości elektronicznej korzystając z publicznych, niezabezpieczonych sieci wi-fi.
- **7.** Nie korzystaj z bankowości elektronicznej na urządzeniach publicznych np. w kafejkach czy hotelach.
- 8. Czytaj potwierdzenia SMS przed zatwierdzeniem transakcji płatniczej.
- **9.** Regularnie aktualizuj system, aplikacje, przeglądarkę oraz oprogramowanie antywirusowe.
- **10.** Nie podłączaj do swojego sprzętu zewnętrznych nośników danych typu. Pendrive, co do których bezpieczeństwa nie masz pewności.

# ZOSTAŃ AMBASADOREM KAMPANII















# Stowarzyszenie MANKO Międzynarodowy Instytut Rozwoju Społecznego

Os. Urocze 12, 31-953 Kraków

**└** tel. +48 12 429 37 28 **└** tel. +48 12 644 59 22

★ kontakt@manko.pl

www.niedajmysieoszukac.pl

www.facebook.com/StopManipulacjiNieDajSieOszukac